UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/087,807	03/05/2002	Masashi Mitomo	1341.1102CIP	5215

21171 7590 11/16/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
REID, CHERYL M	

ART UNIT	PAPER NUMBER
2142	

DATE MAILED: 11/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/087,807	MITOMO ET AL.	
	Examiner	Art Unit	
	Cheryl M. Reid	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-36 and 38-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-36 and 38-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-4,6-36, 38-66 have been examined.

Response to Arguments

2. Applicant's arguments with respect to claims 1, 33,65-66 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1,2, 33, 34 and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cabrera (Statistical Traffic Modeling for Network Intrusion Detection) in view of Cannady (Artificial Neural Networks for Misuse Detection) in view of Dettinger et al (US 6928554) in view of Ontiverso et al (US 20020107953) in view of Fuh et al (US 6609154).

4. In regards to claims 1, 33, 65, Cabera teaches of : an illegal pattern database with stores patterns of illegal accesses to the server (Introduction, Page 1), wherein the patterns of illegal accesses are "attack signatures." Cabera doesn't explicitly teach of

the remaining limitations. In an analogous art, Cannady teaches of a pattern determination unit which estimates the legality of an access request based on the illegal access patterns stored in the illegal pattern database and on a predetermined pattern estimation rules (Background, 3rd paragraph, Current Approaches to Intrusion Detection, 1st paragraph). Cannady does not explicitly teach of the remaining limitations. In an analogous art, Dettinger teaches of a pattern determination unit, wherein Examiner is interpretating "pattern determination unit,", as any unit which makes a determination because this gives the broadest reasonable interpretation, which determines whether each access request is to be transmitted to the server based on estimation (analysis), (col 11, lines 45-50, col 12, lines 45-60) but does not teach of based on predetermined pattern determination rule, wherein Examiner is interpreting "predetermined pattern determination rule," as " predetermined rules," because this interpretation gives the broadest reasonable interpretation. In an analogous art, Ontiveros teaches on this aspect (paragraph 0004). Ontiveros alludes to a transmission unit(firewall, paragraph 0004) but does not give explicitly details. In an analogous art, Fuh teaches of an transmission control (firewall) which controls transmission of the access request based on determination result of the pattern determination unit, wherein the pattern determination unit (Authentication Proxy) determines if the user's patterns (IP address, login, col 3 lines 30-40) is consistent with the patterns' stored in the profile database, so as to transmit the access request to the server when the access request is estimated to be legal, wherein estimated to be legal if user is authorized to use the system, and so as to reject transmission of the access request to the server and so as

to abandon the request when the access request is estimated to be illegal (col 7, lines 50-67, col 8, lines 5-30, col 9, lines 45-67). It would have been obvious to one of ordinary skill in the arts at the time of invention to incorporate the above teachings because the inventions are analogous art (i.e. relates to preventing unauthorized access to system resources). One of ordinary skill in the art at the time of invention would have been motivated to incorporate the above modifications because it would result in a more efficient intrusion detection/prevention system which would prevent unauthorized access to network resources. Ontiveros (paragraph 0003) and Fur(col 1, lines 20-30) teaches that this is a desirable feature of network systems.

5. The rejections of claim 2 and 34 were set forth in a previous office action mailed on 4/21/05.

6. Claim 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cabrera (Statistical Traffic Modeling for Network Intrusion Detection) in view of Cannady (Artificial Neural Networks for Misuse Detection) in view) of Fuh et al (US 6609154).

7. In regard to claim 66, Cabera teaches of : an illegal pattern database with stores patterns of illegal accesses to the server (Introduction, Page 1), wherein the patterns of illegal accesses are "attack signatures." Cabera doesn't explicitly teach of the remaining limitations. In an analogous art, Cannady estimating the legality of an access request based on the illegal access patterns stored in the illegal pattern

database and on a predetermined pattern estimation rules (Background, 3rd paragraph, Current Approaches to Intrusion Detection, 1st paragraph). Cannady does not explicitly teach of the remaining limitations. Fur teaches of receiving a request for access (col 7, lines 25-30), determining whether the access request is to be transmitted to the server based on the estimate of the legality of the access request (col 7, lines 50-55, , col 8, lines 5-30, col 9, lines 45-67).). It would have been obvious to one of ordinary skill in the arts at the time of invention to incorporate the above teachings because the inventions are analogous art (i.e. relates to preventing unauthorized access to system resources). One of ordinary skill in the art at the time of invention would have been motivated to incorporate the above modifications because it would result in a more efficient intrusion detection/prevention system which would prevent unauthorized access to network resources. Ontiveros (paragraph 0003) and Fur(col 1, lines 20-30) teaches that this is a desirable feature of network systems.

8. Claims 3-4,6-15,16-19,26-30,35-36, 38-47,48-51,58-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cabrera (Statistical Traffic Modeling for Network Intrusion Detection) in view of Cannady (Artificial Neural Networks for Misuse Detection) in view of Dettinger et al (US 6928554) in view of Ontiverso et al (US 20020107953) in view of Fuh et al (US 6609154) as applied above to claim 1, and further in view of Carter.

9. The rejections of claims 3-4,6-15,16-19,26-30,35-36, 38-47,48-51,58-62 were set forth in a previous office action mailed on 4/21/05.

10. Claims 31-32 and 63 –64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cabrera (Statistical Traffic Modeling for Network Intrusion Detection) in view of Cannady (Artificial Neural Networks for Misuse Detection) in view of Dettinger et al (US 6928554) in view of Ontiverso et al (US 20020107953) in view of Fuh et al (US 6609154) as applied above to claim 1, and further in view of Carter and Cahill.

11. The rejections of claims 31-32 and 63-64 were set forth in a previous office action mailed on 4/21/05.

12. Claims 20-21 and 52-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cabrera (Statistical Traffic Modeling for Network Intrusion Detection) in view of Cannady (Artificial Neural Networks for Misuse Detection) in view of Dettinger et al (US 6928554) in view of Ontiverso et al (US 20020107953) in view of Fuh et al (US 6609154) as applied above to claim 1, and further in view of Kashani.

13. The rejections of claims 20-21 and 52-53 were set forth in a previous office action mailed on 4/21/05.

14. Claims 22-25 and 54-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cabrera (Statistical Traffic Modeling for Network Intrusion

Detection) in view of Cannady (Artificial Neural Networks for Misuse Detection) in view of Dettinger et al (US 6928554) in view of Ontiverso et al (US 20020107953) in view of Fuh et al (US 6609154) as applied above to claim 1, and further in view of Carter and Kashani.

15. The rejections of claims 22-25 and 54-57 were set forth in a previous office action mailed on 4/21/05.

Conclusion

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cheryl M. Reid whose telephone number is 571 272 3903. The examiner can normally be reached on Mon- Fri (7-3:30).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cmr

BEATRIZ PRIETO
PRIMARY EXAMINER